Box 2.4

THE IMPORTANCE OF TECHNOLOGY PROVIDER RISK MANAGEMENT IN THE FINANCIAL SECTOR

It is a fact that financial institutions around the world rely on external providers for the delivery of their services. The agreements with these third parties are often complex and may involve various providers located in different jurisdictions. This trend was augmented by the COVID-19 pandemic, which forced institutions to quickly adopt technology services provided by third parties in order to continue offering their services to customers. This increased institutions' exposure surface and thus the operational risk they face.

Moreover, it is common for external technology service providers to offer their services through an outsourcing chain, where at each link a different third party provides one part of the service. The complexity of these provider chains makes management difficult and reduces the risk mitigation capacity of both institutions and supervisory or resolution authorities, as it is extremely difficult to identify all the participants involved and, therefore, very difficult to properly assess the potential impact of an incident or the disruption of the service provided by one of them, not only on a given institution, but on the financial sector as a whole.

In recent years the various European authorities, concerned about these risks, have issued regulations to mitigate the risk of outsourcing —European Banking Authority (EBA) Guidelines EBA/GL/2019/02 on outsourcing arrangements and Banco de España Circulars 2/2016 and 3/2022, among others— which both institutions and providers have been incorporating into their arrangements. Given their significance for enabling institutions to adequately manage risks, all three regulations establish various requirements for outsourcing agreements, especially for those that refer to critical services or functions, such as including access and audit right clauses for the institution and for the supervisor or termination and exit clauses. Consequently, the assessment of these arrangements on critical services or functions has been incorporated into institutions' microprudential supervision.

However, supervisory authorities and regulators see a need to broaden the regulatory scope to include all third-party relationships and, in particular, to focus on the oversight of critical service providers to the financial sector. This is illustrated by the initiatives of the European Supervisory Authorities —EBA, European Securities and Markets Authority and European Insurance and Occupational Pensions Authority— to compile technological third-party registers, or the Financial Stability Board's public consultation on issues relating to outsourcing and third-party relationships, which, among other aspects, highlights the need to establish a common terminology (lexicon) with global consistent definitions.

In addition, the forthcoming implementation of the Digital Operational Resilience Act (DORA) will establish additional requirements for institutions and a framework for the oversight of critical technology providers for the entire European financial sector.

Why are we so concerned about the potential risk posed by these external technology service providers? The answer is immediate: in addition to the risks associated with this dependence, there is the threat posed by supply chain attacks, which have proliferated in recent years, usually targeting suppliers and software developers, with the aim of reaching a company through its third-party relationships. The number of potential victims in such an attack can be significant, sometimes affecting thousands of companies.

These attacks are harder to detect if suppliers do not implement a proactive security approach, with adequate security policies and detection and response tools that make it possible to identify and act upon suspicious activity. Also, it is important that suppliers have in place an incident response procedure for supply chain attacks, and that this ensures that institutions and their customers are notified, where appropriate, with accurate and timely information.

In conclusion, in order to determine an institutions' level of exposure it is essential to identify, supervise and manage the risks arising from the relationships with its external technology service providers.